Available online at www.sciencedirect.com
ScienceDirect
European Journal of Combinatorics 28 (2007) 36–42
European Journal of Combinatorics
www.elsevier.com/locate/ejc

Blocking sets of external lines to a conic in $PG(2, q)$, q even[☆]

Massimo Giulietti

Dipartimento di Matematica e Informatica, Università degli Studi di Perugia Via Vanvitelli 1, 06123, Perugia, Italy

Received 23 May 2004; accepted 4 October 2004
Available online 11 November 2005

Abstract

All point-sets of minimum size in $PG(2, q)$, q even, that meet every external line to a conic in $PG(2, q)$ are classified.

MSC: 51E21

1. Introduction

Let $\mathcal{C}$ be an irreducible conic in the desarguesian plane $PG(2, q)$. There are exactly $(q-1)q/2$ lines of $PG(2, q)$ which do not intersect $\mathcal{C}$ at any point in $PG(2, q)$. Each of these lines is called an *external line* to $\mathcal{C}$. A point-set $\mathcal{K}$ in $PG(2, q)$ which blocks the external lines to $\mathcal{C}$, i.e. incident with each external line to $\mathcal{C}$, is called a *blocking set of external lines* to $\mathcal{C}$. The main problem is to find the minimum size for blocking sets of external lines to a conic, and to give a geometric construction for those which attain such a limit. This problem has been solved so far for odd q by proving that the minimum size is $q - 1$, and that for $q \geq 9$ any blocking set of external lines to $\mathcal{C}$ of size $q - 1$ consists of a chord r of $\mathcal{C}$ minus the two common points of r and $\mathcal{C}$, see [1].

In this paper we deal with the even order case. We prove that the above result does not hold for even q as two more possibilities for the minimum size occur. Henceforth q is assumed to be a power of 2.

☆ This research was supported by Italian Ministry MIUR, project *Strutture Geometriche, Combinatoria e loro applicazioni*, PRIN 2002–2003, and by GNSAGA.
E-mail address: giuliet@dipmat.unipg.it.

0195-6698/$ - see front matter
doi:10.1016/j.ejc.2004.10.005

Theorem 1.1. *The minimum size of a blocking set of external lines to an irreducible conic $\mathcal{C}$ of $PG(2,q)$ is $q-1$.*

Theorem 1.2. *Let $\mathcal{C}$ be an irreducible conic of $PG(2,q)$, and let N be its nucleus. For a blocking set $\mathcal{K}$ of external lines to $\mathcal{C}$ with $|\mathcal{K}| = q-1$, one of the following occurs:*

(1) *$\mathcal{K}$ consists of the points of a chord r of $\mathcal{C}$, minus the two common points of r and $\mathcal{C}$.*
(2) *$\mathcal{K}$ consists of the points of a tangent line to $\mathcal{C}$, minus the tangency point and N.*
(3) *For q square, $\mathcal{K}$ consists of the points of a Baer subplane Π such that $|\Pi \cap \mathcal{C}| = \sqrt{q}+1$ and $N \in \Pi$, minus N and the common points of $\mathcal{C}$ and Π.*

2. Polynomials vanishing at points uncovered by the lines of a line-conic in $PG(2,q)$, q even

In $PG(2,q)$, a line-conic is defined to be the set $\mathbf{C}$ of all lines in $PG(2,q)$ whose Plücker coordinates satisfy an irreducible quadratic equation over $\mathbb{F}_q$. A line-conic consists of $q+1$ lines, and the points of $PG(2,q)$ are of three types, according to whether the point is uncovered by the lines of $\mathbf{C}$, or covered by either one or two lines of $\mathbf{C}$. The locus of points covered by just one line of $\mathbf{C}$ is a line $\mathcal{N} \notin \mathbf{C}$ which is called the line-nucleus of $\mathbf{C}$. The subgroup G of $PGL(3,q)$ preserving $\mathbf{C}$ also preserves $\mathcal{N}$ and acts on the points of $\mathcal{N}$ as the projective linear group $PGL(2,q)$ on the projective line $PG(1,q)$ over $\mathbb{F}_q$.

Note that if $\mathbf{C}$ is given in its canonical form, i.e. it consists of all lines of equation $a_1X+a_2Y+a_3T=0$ with $a_1^2 = a_2a_3$, then its line-nucleus has equation $X=0$. Furthermore, the points uncovered by the lines of $\mathbf{C}$ are the points $(m, \lambda m^2, 1)$, with $m \in \mathbb{F}_q$, $m \neq 0$, and $\lambda \in C_1$. Here, C_1 stands for the set of those elements $s \in \mathbb{F}_q$ for which the polynomial x^2+x+s has no roots in $\mathbb{F}_q$. In fact, a point $(m, b, 1)$, $b \neq 0$, is uncovered by $\mathbf{C}$ if and only if the polynomial $x^2+x+\frac{b}{m^2}$ has no solution in $\mathbb{F}_q$. Note that every point (u, v, w) with $vw=0$ is covered by the lines of $\mathbf{C}$ as both $Y=0$ and $T=0$ are lines of $\mathbf{C}$.

By duality, a blocking set of external lines to a conic corresponds to a line-set in the dual plane which covers all those points uncovered by the lines of the corresponding line-conic.

Theorem 2.1. *Let $\mathbf{C}$ be a line-conic in $PG(2,q)$, and Γ an algebraic curve defined over the algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$. If Γ passes through every point uncovered by the lines of $\mathbf{C}$, then the order of Γ is at least $q-1$.*

Proof. Assume on the contrary that there exists an algebraic curve Γ defined over $\bar{\mathbb{F}}_q$ of degree d with

$$d < q-1, \tag{1}$$

such that Γ passes through every point uncovered by the lines of $\mathbf{C}$. Let $\mathcal{G}$ denote the set of all such curves Γ. Clearly $\mathcal{G}$ is left invariant by G. Choose a reference system in which $\mathbf{C}$ consists of the lines of equation $a_1X+a_2Y+a_3T=0$ with $a_i \in \mathbb{F}_q$ and $a_1^2 = a_2a_3$. We need the following lemma.

Lemma 2.2. *Every $\Gamma \in \mathcal{G}$ passes through the points of the line-nucleus of $\mathbf{C}$.*

Proof. Since G acts transitively on $\mathcal{N}$ it is enough to prove the statement for $P=(0,0,1)$, that is $f(0,0)=0$ for every polynomial $f(X,Y)$ over $\bar{\mathbb{F}}_q$ of degree d satisfying

$$f(m, \lambda m^2) = 0, \qquad \text{for every } m \in \mathbb{F}_q \setminus \{0\} \qquad \text{and} \qquad \lambda \in C_1.$$

Let $f(X,Y)=\sum a_{ij}X^iY^j$. It is straightforward to see that for every non-zero element $u\in\mathbb{F}_q$, the polynomial

$$f_u(X,Y)=\sum a_{ij}(uX)^i(u^2Y)^j=\sum u^{i+2j}a_{ij}X^iY^j$$

is such that $f_u(m,\lambda m^2)=0$ for any $m\in\mathbb{F}_q$, $m\neq 0$, and for any $\lambda\in C_1$. Clearly, the same holds for the polynomial

$$\bar{f}(X,Y)=\sum_{u\in\mathbb{F}_q^*} f_u(X,Y).$$

Let $\bar{f}(X,Y)=\sum b_{ij}X^iY^j$. Then $b_{ij}=(\sum_{u\in\mathbb{F}_q^*}u^{i+2j})a_{ij}$. By Lemma 6.3 in [3],

$$b_{ij}=\begin{cases}a_{ij} & \text{when either } i=j=0, \text{ or } i+2j=q-1,\\ 0 & \text{otherwise.}\end{cases} \tag{2}$$

This shows that $\bar{f}(X,Y)=a_{00}+\sum b_jX^{q-2j-1}Y^j$, with $b_j\in\mathbb{F}_q$. From (1) and the fact that $\deg\bar{f}(X,Y)\le d$, both $b_0=0$ and $j\le\frac{1}{2}(q-2)$ hold. For every $\lambda\in C_1$, we have $\bar{f}(x,\lambda x^2)=0$ provided that $x\in\mathbb{F}_q$. Hence $a_{00}+\sum_{j=1}^{\frac{1}{2}(q-2)}b_j\lambda^j=0$. This yields that the polynomial $g(T)=a_{00}+\sum_{j=1}^{\frac{1}{2}(q-2)}b_jT^j$ is identically zero, as it has $q/2$ distinct roots. In particular $a_{00}=0$; hence $f(0,0)=0$. This completes the proof of the lemma. □

Lemma 2.2 together with (1) yields that every $\Gamma\in\mathcal{G}$ is reducible as it contains the line-nucleus as a component. Then the curve of degree $d-1$ arising from Γ by removing this line still passes through every point uncovered by the lines of $\mathbf{C}$. But this contradicts the minimality of d. □

Curves of the same degree passing through every point uncovered by the lines of a line-conic of $PG(2,q)$ constitute a linear system. For the minimal degree, we compute the dimension of such a linear system.

Theorem 2.3. *The linear system of algebraic curves of order $q-1$ passing through every point uncovered by the lines of a line-conic of $PG(2,q)$, with q even, has dimension $q-1$. Such points impose independent conditions on the algebraic curves of degree $q-1$ which pass through them.*

Proof. We keep the notation of the proof of Theorem 2.1. Let $\mathcal{V}$ be the linear space over $\mathbb{F}_q$ of the polynomials $f\in\mathbb{F}_q[X,Y]$ such that $\deg(f)\le q-1$ and $f(m,\lambda m^2)=0$, for any $m\in\mathbb{F}_q\setminus\{0\}$ and $\lambda\in C_1$. We need to prove that $\dim_{\mathbb{F}_q}(\mathcal{V})=q$. For any $t\in\mathbb{F}_q$ let

$$\varphi_t(X,Y):=1+(tX+Y+t^2)^{q-1}.$$

Note that $\varphi_t\in\mathcal{V}$, as $t^2+tm+m^2\lambda$ is different from 0 as $\lambda\in C_1$. Write $\varphi_t(X,Y)=\varphi_{t,0}(X,Y)+\varphi_{t,1}(X,Y)+\varphi_{t,q-1}(X,Y)$, with $\varphi_{t,i}(X,Y)$ homogeneous of degree i. We begin by proving the following lemma.

Lemma 2.4. *The set $\mathcal{S}:=\{\varphi_{t,q-1}(X,Y)\mid t\in\mathbb{F}_q\}$ is a basis for the linear space $\mathcal{W}$ of homogeneous polynomials of degree $q-1$ in $\mathbb{F}_q[X,Y]$.*

Proof. Write the polynomial $\varphi_{t,q-1}(x,y)=(tx+y)^{q-1}$ as a linear combination of the usual basis $\{x^iy^{q-1-i}\mid i=0,\dots,q-1\}$ of $\mathcal{W}$. It is easy to see that the coefficients of such a linear

combination are

$$\binom{q-1}{0}t^{q-1}, \binom{q-1}{1}t^{q-2}, \binom{q-1}{2}t^{q-3}, \ldots, \binom{q-1}{q-2}t, 1.$$

Put these coefficients in a $q \times q$ matrix A. Then, apart from the nonzero factor

$$c = \prod_{i=0}^{q-1}\binom{q-1}{i},$$

the determinant of A is of Vandermonde type with elements w^i, where $i = 0, \ldots, q-1$ and w is a primitive element of $\mathbb{F}_q$, which is well known to be different from 0. □

Let a be any element in $\mathcal{V}$, and write

$$a(x, y) = \Psi_0(x, y) + \cdots + \Psi_{q-1}(x, y)$$

where $\Psi_i(x, y)$ is a homogeneous polynomial of degree i. By the above lemma,

$$\Psi_{q-1}(x, y) = \sum_{t\in\mathbb{F}_q} \lambda_t \varphi_{t,q-1}(x, y)$$

for suitable $\lambda_t \in \mathbb{F}_q$. Now assume that the polynomial $a(x, y) - \sum_{t\in\mathbb{F}_q} \lambda_t \varphi_t(x, y)$ is not identically zero. Then it has degree $q-2$ and belongs to $\mathcal{V}$, contradicting Theorem 2.1. Therefore

$$a(x, y) = \sum_{t\in\mathbb{F}_q} \lambda_t \varphi_t(x, y).$$

This proves that $\dim_{\mathbb{F}_q}(\mathcal{V}) \le q$. On the other hand, $\dim_{\mathbb{F}_q}(\mathcal{V}) \ge q$ as $\mathcal{V}$ is obtained by imposing $\frac{q^2-q}{2}$ linear conditions on the $(\frac{q^2+q}{2})$-dimensional linear space of all polynomials in $\mathbb{F}_q[x, y]$ of degree at most $q-1$. □

3. A subgroup of $PSL(2, q)$ associated with a blocking set of external lines

Let t be a line in the line-conic $\mathbf{C}$, and $\mathbf{B}$ a line-set of size $q-1$ which covers all points uncovered by the lines of $\mathbf{C}$. We begin by showing how to associate with $\mathbf{B}$ a set of involutions of $PSL(2, q)$ viewed as the linear projective group of t. The subgroup generated by these involutions will play an important role in the proof of Theorem 1.2.

Again, $\mathbf{C}$ is assumed to be in its canonical form, that is $\mathbf{C}$ consists of the lines of equation $a_1X + a_2Y + a_3T = 0$ with $a_i \in \mathbb{F}_q$ and $a_1^2 = a_2a_3$. Furthermore, assume t to be the line of equation $T = 0$. With any line $\ell \notin \mathbf{C}$ we may associate an involution η_ℓ in $PSL(2, q)$. If ℓ is the line of equation $X = kT$, $k \in \mathbb{F}_q \setminus \{0\}$, put

$$\eta_\ell(1, \gamma, 0) = (1, \gamma + k, 0), \qquad \eta_\ell(0, 1, 0) = (0, 1, 0),$$

whereas if ℓ has equation $Y = \alpha X + \beta T$, put

$$\eta_\ell(1, \gamma, 0) = \begin{cases} \left(1, \dfrac{\alpha\gamma + \beta}{\alpha + \gamma}, 0\right), & \text{for } \gamma \neq \alpha \\ (0, 1, 0), & \text{for } \gamma = \alpha \end{cases}, \qquad \eta_\ell(0, 1, 0) = (1, \alpha, 0).$$

As l ranges over $\mathbf{B}$, then the corresponding η_ℓ generate a subgroup $\mathcal{G}_\mathbf{B}$ of $PSL(2, q)$. Some useful properties of $\mathcal{G}_\mathbf{B}$ are stated in the following lemmas.

Lemma 3.1. *Let Λ be the point-set in the line t of equation $T = 0$ which comprises $(0, 1, 0)$ and all points covered by some line in $\mathbf{B}$. Then $\mathcal{G}_{\mathbf{B}}$ fixes Λ setwise.*

Proof. As we have shown in the proof of Theorem 2.3, the totally reducible algebraic curve whose components are the lines in $\mathbf{B}$ has the equation

$$F_{\mathbf{B}}(X, Y, T) := \sum_{s\in\mathbb{F}_q} \lambda_s (T^{q-1} + (tX + Y + t^2T))^{q-1} = 0,$$

for some $\lambda_s \in \mathbb{F}_q$. Let $\lambda = \sum_{s\in\mathbb{F}_q} \lambda_s$. Note that a point $(1, v, 0)$ belongs to Λ if and only if $\lambda = \lambda_v$. Now fix $P \in \Lambda$ and $\ell \in \mathbf{B}$. If either $P = (0, 1, 0)$ or $P = \ell \cap t$, then $\eta_\ell(P) \in \Lambda$ by definition. Assume that $P = (1, v, 0)$ for some $v \in \mathbb{F}_q$ with $\lambda + \lambda_v = 0$, $P \notin \ell$.

Two cases are distinguished. First, we assume that $\ell : Y = \alpha X + \beta T$. Note that the point $Q = (\frac{v^2+\beta}{v+\alpha}, v\frac{v^2+\beta}{v+\alpha} + v^2, 1) \in \ell$. As $(t\frac{v^2+\beta}{v+\alpha} + v\frac{v^2+\beta}{v+\alpha} + v^2 + t^2)^{q-1}$ is equal to 1 for all $s \in \mathbb{F}_q$ but $s = v$, $s = \frac{\alpha v+\beta}{v+\alpha}$, $F_{\mathbf{B}}(\frac{v^2+\beta}{v+\alpha}, v\frac{v^2+\beta}{v+\alpha} + v^2, 1) = 0$ yields $\lambda_v = \lambda_{\frac{\alpha v+\beta}{v+\alpha}}$. Hence $\eta_\ell(P) \in \Lambda$, as $\lambda_{\frac{\alpha v+\beta}{v+\alpha}} = \lambda_v = \lambda$. Assume now that $\ell : X = kT$. The point $Q = (k, vk + v^2, 1)$ belongs to ℓ. As in the previous case, $F_{\mathbf{B}}(k, vk + v^2, 1) = 0$ yields $\lambda_v = \lambda_{v+k}$, and hence $\eta_\ell(P) \in \Lambda$. □

Lemma 3.2. *If $\mathcal{G}_{\mathbf{B}}$ fixes one point P on $T = 0$, then $\mathbf{B}$ consists of $q - 1$ concurrent lines. More precisely, if $P = (0, 1, 0)$ then $\mathbf{B}$ is the set of lines $X = kT$, $k \in \mathbb{F}_q$, $k \neq 0$; otherwise there exists $\beta_0 \in \mathbb{F}_q$ such that $\mathbf{B}$ is the set of lines of equation $Y = \alpha X + \beta_0^2$, $\alpha \in \mathbb{F}_q$, $\alpha \neq \beta_0$.*

Proof. It is straightforward to check that η_ℓ fixes exactly one point on $T = 0$, namely $(0, 1, 0)$ when $\ell : X = kT$, $k \in \mathbb{F}_q$, $k \neq 0$, and $(1, \beta^{q/2}, 0)$ when $\ell : Y = \alpha X + \beta T$. Hence if $P = (0, 1, 0)$, any $\ell \in \mathbf{B}$ is of type $X = kT$ with $k \neq 0$. On the other hand, if $P = (1, \beta_0, 0)$, $\beta_0 \in \mathbb{F}_q$, then any $\ell \in \mathbf{B}$ is of type $Y = \alpha X + \beta_0^2 T$ with $\alpha \in \mathbb{F}_q$, $\alpha \neq \beta_0$. □

Lemma 3.3. *If there exist two points $P = (1, \gamma, 0)$, $P' = (1, \gamma', 0)$ on $T = 0$ such that every involution in $\mathcal{G}_{\mathbf{B}}$ interchanges P and P', then $\mathbf{B}$ consists of $q - 1$ lines through $Q = (\gamma + \gamma', \gamma\gamma', 1)$.*

Proof. Let η_ℓ be such that $\eta_\ell(1, \gamma, 0) = (1, \gamma', 0)$. Then it is easy to see that either $\ell : Y = \alpha X + \beta T$, $\alpha \in \mathbb{F}_q$, $\alpha^2 \neq \beta$, and $\gamma\gamma' + \alpha(\gamma + \gamma') + \beta = 0$, or $\ell : X = kT$, with $k = \gamma + \gamma'$. In both cases ℓ passes through the point $Q = (\gamma + \gamma', \gamma\gamma', 1)$, and the lemma is proved. □

4. Proof of Theorems 1.1 and 1.2

Theorem 1.1 is the dual of Theorem 2.1.

To prove Theorem 1.2, the classification of all subgroups of $PSL(2, q)$ is needed; see [2, p. 213].

Theorem 4.1. *For $q = 2^m$, a complete list of subgroups of $PSL(2, q)$, is as follows:*

(a) *cyclic groups of order d with $d \mid (q \pm 1)$;*
(b) *elementary abelian groups of order 2^k with $k \leq m$;*
(c) *dihedral groups of order $2d$ with $d \mid (q \pm 1)$;*
(d) *groups of order $2^k s$ with $s|(2^k - 1)$ and $s|(2^m - 1)$ which are semidirect products of an elementary abelian group of order 2^k with a cyclic group of order $s > 1$;*
(e) *projective linear groups $PSL(2, 2^k)$ with $k|m$.*

Now we are in a position to prove Theorem 1.2.

Proof of Theorem 1.2. Let $\mathcal{C}$ be the conic given in its canonical form $YT = X^2$. With each point P in $\mathcal{K}$ we associate an involution in $\eta_P \in PSL(2,q)$ as follows: if $P = (\alpha, 1, \beta)$, then put $\eta_P = \begin{pmatrix} \alpha & \beta \\ 1 & \alpha \end{pmatrix}$, otherwise $P = (1,0,k)$ and put $\eta_P = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$. Let G be the subgroup of $PSL(2,q)$ generated by η_P with P ranging over $\mathcal{K}$. In the dual plane, G coincides with the group $\mathcal{G}_{\mathbf{B}}$ defined in the previous section, where $\mathbf{B}$ is the line-set corresponding to $\mathcal{K}$. In this setting, $PSL(2,q)$ is the projective linear group of the line t of equation $T = 0$.

According to Theorem 4.1 a number of cases can occur for G. We treat them separately, focusing on the action of G on t. Note that, by Lemma 3.1, G is an intransitive subgroup of $PSL(2,q)$.

G is neither of type (a), as it contains $q - 1 > 2$ involutions, nor of type (d), as it is generated by involutions. If G is of type (b), then G fixes a point; hence the configuration given in case (2) of Theorem 1.2 can only occur for $\mathcal{K}$ by the dual of Lemma 3.2. Assume G to be of type (c). Since G contains $q - 1$ involutions, either G has order $2(q+1)$ and G is transitive, or it has order $2(q-1)$ and G swaps two points. The former case does not occur, G being intransitive. In the latter case, the dual of Lemma 3.3 forces $\mathcal{K}$ to be the configuration described in (1) of Theorem 1.2.

We are left with the case where q is a square, and G is isomorphic to $PSL(2,\sqrt{q})$. Since $PSL(2,q)$ has just one conjugacy class of subgroups isomorphic to $PSL(2,\sqrt{q})$, we may assume G to be $gPSL(2,\sqrt{q})g^{-1}$ for some $g \in PSL(2,q)$ [2, Sec. II.8].

Note that $h \in PSL(2,\sqrt{q})$ is an involution if and only if h is defined either by $\begin{pmatrix} \lambda & \mu \\ 1 & \lambda \end{pmatrix}$, $\lambda, \mu \in \mathbb{F}_{\sqrt{q}}$, $\lambda^2 \neq \mu$ or by $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, $k \in \mathbb{F}_{\sqrt{q}}$, $k \neq 0$.

Assume at first that g is defined by $\begin{pmatrix} a_{11} & a_{12} \\ 1 & a_{22} \end{pmatrix}$. Then it is straightforward to check that the involutions in $gPGL(2,\sqrt{q})g^{-1}$ are those elements defined by

$$\begin{pmatrix} \lambda(a_{12}+a_{11}a_{22})+\mu a_{11}+a_{12}a_{22} & \mu a_{11}^2 + a_{12}^2 \\ \mu + a_{22}^2 & \lambda(a_{12}+a_{11}a_{22})+\mu a_{11}+a_{12}a_{22} \end{pmatrix},$$

for $\lambda, \mu \in \mathbb{F}_{\sqrt{q}}$, $\lambda^2 \neq \mu$, together with those defined by

$$\begin{pmatrix} ka_{11}+a_{12}+a_{11}a_{22} & ka_{11}^2 \\ k & ka_{11}+a_{12}+a_{11}a_{22} \end{pmatrix}, \qquad k \in \mathbb{F}_{\sqrt{q}}, k \neq 0.$$

Hence, the points in $\mathcal{K}$ are those of coordinates $(\alpha, 1, \beta)$ with either

$$\alpha = \frac{\lambda(a_{12}+a_{11}a_{22})+\mu a_{11}+a_{12}a_{22}}{\mu + a_{22}^2}, \qquad \beta = \frac{\mu a_{11}^2 + a_{12}^2}{\mu + a_{22}^2},$$

with $\lambda, \mu \in \mathbb{F}_{\sqrt{q}}$, $\lambda^2 \neq \mu$, $\mu \neq a_{22}^2$

or

$$\alpha = \frac{ka_{11}+a_{12}+a_{11}a_{22}}{k}, \qquad \beta = a_{11}^2, \qquad \text{with } k \in \mathbb{F}_{\sqrt{q}}, k \neq 0,$$

together with the points $(1,0,h)$ with

$$h = \frac{a_{11}^2 a_{22}^2 + a_{12}^2}{\lambda(a_{11}a_{22}+a_{12}) + a_{11}a_{22}^2 + a_{12}a_{22}}, \qquad \lambda \in \mathbb{F}_{\sqrt{q}}, \lambda \neq a_{22}.$$

Now let Φ be linear transformation of $PG(2,q)$ defined by

$$\Phi : (X,Y,T) \to (X(a_{12}+a_{11}a_{22})+Ya_{11}+Ta_{12}a_{22}, Y+Ta_{22}^2, Ya_{11}^2+Ta_{12}^2),$$

and let $\Pi = \Phi(PG(2,\sqrt{q}))$. Then Π is a Baer subplane of $PG(2,q)$ containing $\sqrt{q}+1$ points of $\mathcal{C}$, namely the points $\Phi(P)$, with $P=(\omega,1,\omega^2)$, $\omega \in \mathbb{F}_{\sqrt{q}}$ or $P=(0,0,1)$. The nucleus $N=(1,0,0)$ of $\mathcal{C}$ is fixed by Φ, and hence it belongs to Π as well. Moreover, it is easy to see that $\mathcal{K}$ coincides with the set of points of Π not in $\mathcal{C}\cup\{N\}$.

Now, let g be defined by $\begin{pmatrix} a_{11} & a_{12} \\ 0 & 1 \end{pmatrix}$. Then, arguing as above, it is straightforward to check that the points in $\mathcal{K}$ are $(\alpha,1,\beta)$ with

$$\alpha = \lambda a_{11}+a_{12}, \qquad \beta = \mu a_{11}^2 + a_{12}^2, \qquad \text{with } \lambda,\mu \in \mathbb{F}_{\sqrt{q}}, \lambda^2 \neq \mu,$$

together with the points $(1,0,ka_{11})$, $k \in \mathbb{F}_{\sqrt{q}}$, $k \neq 0$. Let Φ' be a linear transformation of $PG(2,q)$ defined by

$$\Phi'(X,Y,T) = (Xa_{11}+Ta_{12}, T, Ya_{11}^2+Ta_{12}^2),$$

and let $\Pi' = \Phi'(PG(2,\sqrt{q}))$. Then Π' is a Baer subplane of $PG(2,q)$ containing $\sqrt{q}+1$ points of $\mathbf{C}$, namely the points $\Phi'(P)$, with $P=(\omega,1,\omega^2)$, $\omega \in \mathbb{F}_{\sqrt{q}}$ or $P=(0,0,1)$. The nucleus $N=(1,0,0)$ of $\mathcal{C}$ is fixed by Φ', and hence it belongs to Π' as well. Again, the proof that $\mathcal{K}$ coincides with the set of points of Π' not in $\mathcal{C}\cup\{N\}$ is straightforward. □

References

[1] A. Aguglia, G. Korchmáros, Blocking sets of external lines to a conic in $PG(2,q)$, q odd, Combinatorica (in press).
[2] B. Huppert, Endliche Gruppen I, Springer, Berlin, Germany, 1967.
[3] R. Lidl, H. Niederreiter, Finite Fields, Addison Wesley, Reading, MA, USA, 1983, Cambridge University Press, 1984.